UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: **COMMISSIONER FOR PATENTS**
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,047	08/23/2000	Alexandr Andreevich Moldovyan	P65855US0	4150

			EXAMINER
136	7590	05/23/2006	LANIER, BENJAMIN E

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/622,047	MOLDOVYAN ET AL.
	Examiner	Art Unit
	Benjamin E Lanier	2132

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3 and 5* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3 and 5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☒ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 12 April 2006 has been entered.

Response to Amendment

2.   Applicant's amendment filed 12 April 2006 amends claims 1, 3, cancels claim 3, and

adds claim 5. Applicant's amendment has been fully considered and has been entered.

Response to Arguments

3.   Applicant's arguments filed 12 April 2006 have been fully considered but they are not

persuasive. Applicant's argument that Schneier does not disclose prior to carrying out said two-

place operation on an I-th data subblock and a subkey, an operation of permuting subkey bits is

performed on the subkey depending on the value of a j-th data subblock, where i is not equal to j

is not persuasive because Schneier discloses the DES algorithm wherein a 64-bit block of plain

text is split into a right half and a left half (Page 270), which meets the limitation of breaking

down a data block into $N \geq 2$ subblocks. The encryption key is broken up into 16 subkeys (Figure

12.1), which meets the limitation of generating an encryption key in the form of a set of subkeys.

There are 16 rounds of identical operations in which the data are combined with the key (Page

270 & Figure 12.1). The operations performed are exclusive or (Xor) operations (Page 270 &

Figure 12.1), which meets the limitation of alternatively converting said data subblocks by

performing a two-place operation on the data subblock and the subkey because figure 12.1 shows

the exclusive or operation being performed on the subblock and the subkey. An exclusive or

(Xor) operation is a two-place operation. In each round the key bits are shifted depending on a

subblock (Page 270 & Figure 12.1), which meets the limitation of prior to carrying out said two-

place operation on an I-th data subblock and a subkey, an operation of permuting subkey bits is

performed on the subkey depending on the value of the j-th data subblock where i is not equal to

j, because figure 12.1 shows that the data subblock Lo is exclusive or'd with the result of the

permutation function on subkey Ki that depends on data subblock Ro. Therefore, from figure

12.1 (looking at one round for an example), Lo would meet the limitation of the i-th data

subblock, Ro would meet the limitation of the j-th data subblock, K1 would meet the limitation

of the subkey being permuted, and function f would meet the limitation of the permutation

function.

4.   Applicant's arguments that Schneier does not disclose permuting subkey bits depending

on data subblock is not persuasive because Schneier clearly discloses that the permutation

function f, performs a permutation on the subkey because Schneier routines refers to the

"permuted key" (Page 270). This function is clearly dependant on data subblock because the

permutation function f, takes as it's inputs (referring specifically to the calculation for R1),

subkey K1 and data subblock Ro. Therefore, the permutation function that is performed on

subkey K1 is done so dependent upon data subblock Ro that is also taken as an input to the

permutation function. Applicant's description of Schneier (last paragraph of page 4 through page

5) does not detail the permutation function in particular as Applicant is alleging. Page 5 is

detailing the broadening of the L subblock, which is clearly not part of the permutation function f

that takes only subkey Ki and data subblock Ro. Applicant further details the exclusive or

function, which also is not part of the permutation function f, but is instead the claimed two-

place operation performed on the subblock L. Applicant then goes on to describe the s-box and

p-box permutations of the DES algorithm that have nothing to do with the permutation function f

that takes in only subkey K1 and data subblock Ro as inputs, and have not been relied upon to

teach the claimed invention.

Applicant's last argument also does not take into account that Schneier describes the permutation

function f, which provides a "permuted key", takes in subkey K1 and data subblock Ro

(calculation of R1 used as the example) as inputs. Therefore, the permutation of subblock K1 is

dependant on data subblock Ro.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

6.   Claims 1, 3 rejected under 35 U.S.C. 102(b) as being anticipated by Schneier. Referring

to claim 1, Schneier discloses the DES algorithm wherein a 64-bit block of plain text is split into

a right half and a left half (Page 270), which meets the limitation of breaking down a data block

into $N \geq 2$ subblocks. The encryption key is broken up into 16 subkeys (Figure 12.1), which meets

the limitation of generating an encryption key in the form of a set of subkeys. There are 16

rounds of identical operations in which the data are combined with the key (Page 270 & Figure

12.1). The operations performed are exclusive or (Xor) operations (Page 270 & Figure 12.1),

which meets the limitation of alternatively converting said data subblocks by performing a two-place operation on the data subblock and the subkey because figure 12.1 shows the exclusive or operation being performed on the subblock and the subkey. An exclusive or (Xor) operation is a two-place operation. In each round the key bits are shifted depending on a subblock (Page 270 & Figure 12.1), which meets the limitation of prior to carrying out said two-place operation on an I-th data subblock and a subkey, an operation of permuting subkey bits is performed on the subkey depending on the value of the j-th data subblock where i is not equal to j, because figure 12.1 shows that the data subblock Lo is exclusive or'd with the result of the permutation function on subkey Ki that depends on data subblock Ro. Therefore, from figure 12.1 (looking at one round for an example), Lo would meet the limitation of the i-th data subblock, Ro would meet the limitation of the j-th data subblock, K1 would meet the limitation of the subkey being permuted, and function f would meet the limitation of the permutation function.

Referring to claim 3, Schneier discloses that each round the subkey bits are shifted depending on a subblock as discussed above (Page 270 & Figure 12.1), which meets the limitation of an operation of an operation of cyclic offsetting subkey bits depending on the j-th subblock is used as the j-th subblock-dependent operation of permuting subkey bits because the permutation function on the subkeys are performed each round and that would be considered cyclical.

Referring to claim 5, Schneier discloses that the subkeys are shifted as a result of a permutation function that depends on the j-th data subblock as discussed above (Page 270 & Figure 12.1). In the later rounds of the algorithm (see figure 12.1, specifically the calculation for R2), the permutation function operates on subkey K2 dependant upon the result of R1 data block

calculation. The R1 data block calculation involved subkey K1, and therefore, the calculation of

R2 also includes data from subkey K1, which meets the limitation of the operation of permuting

subkey bits is performed on one of said set of subkeys depending on the value of the j-th data

subblock, where i is not equal to j, and the value of another subkey.

Conclusion

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier